CONTROL UNIT

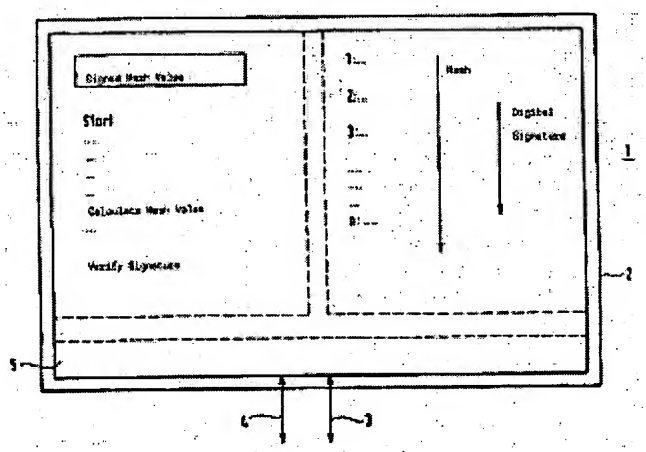
Patent number: WO03001348
Publication date: 2003-01-03
Inventor: SCHWAN OLAF (DE); UEBELACKER HUBERT (DE); LINDLBAUER MARC (DE)
Applicant: GIESECKE & DEVRIENT GMBH (DE); SECARTIS AG (DE); SCHWAN OLAF (DE); UEBELACKER HUBERT (DE); LINDLBAUER MARC (DE)
Classification:
- international: ***G11C16/22;* G11C16/06;** (IPC1-7): G06F1/00
- european: G11C16/22
Application number: WO2002EP06399 20020611
Priority number(s): DE20011028305 20010612

Also published as:
WO03001348 (A3)
EP1399797 (A3)
EP1399797 (A2)
US2004187035 (A1)
DE10128305 (A1)

Cited documents:
EP0455174
DE19512266

Abstract of **WO03001348**

The invention relates to a control unit for technical arrangements, devices and/or machines with a microprocessor, comprising a programmable memory and a housing which surrounds the microprocessor and the programmable memory. Data lines extend from the housing for connection to an external device in order for data to be written into the programmable memory. Said control unit is disposed within the housing in such a manner that when the housing is opened, the operability of the control unit is at least partially impaired. The control unit also comprises a control device which checks write access when data is written into the programmable memory by means of the data lines in terms of authorisation. If the write access authorisation thus monitored is correct, then data can be written into the programmable memory.



CONTROL UNIT

Description of **WO03001348**

Steuereinheit Die Erfindung betrifft eine Steuereinheit für technische Anlagen, Geräte und/oder Maschinen mit einem Mikroprozessor, mit einemprogrammierba- ren Speicher, mit einem Gehäuse und mit zumindest einer aus dem Gehäuse herausführenden Datenleitung zur Verbindung mit einer externenEinrich- tung zum Schreiben von Daten in den programmierbaren Speicher.

Derartige auf Mikrocontrollern basierende Steuereinheiten werden mittlerweile in sehr vielen Maschinen und Geräten, beispielsweise im Kraftfahrzeug oder in der Consumer-Elektronik etc., eingesetzt. Das vom Mikroprozessor benötigte Steuerungsprogramm ist hierbei üblicherweise in einem programmierbaren Speicher hinterlegt. In vielen Fällen handelt es sich hierbei zumindest teilweise um einen frei programmierbaren, wieder löschbaren und überschreibbaren Speicher. Die Steuereinheit kann dann jederzeit kunden-und anwendungsspezifisch angepasst werden, indem die hierfür benötigten Daten und gegebenenfalls auch komplette Programmabläufe geändert werden. Diese nachträgliche Änderung erlaubt insbesondere auch eine spätere Verbesserung oder Aktualisierung desSteuerungsprogramms. Insbesondere ist es auf diese Weise möglich, über Veränderungen der Steuerungssoftware beispielsweise auch den Funktions-und/oder den Leistungsumfang der Steuereinheit und damit der gesamten technischen Anlagen des Geräts oder der Maschine nachträglich zu modifizieren. DieUmprogram- mierung erfolgt üblicherweise dadurch, dass eine externe Einrichtung an eine aus dem Gehäuse herausführende Datenleitung angeschlossen wird und über die Datenleitung dann die erforderlichen Daten in den programmierbaren Speicher geschrieben werden. Bei der externen Einrichtung handelt es sich oft um ein spezielles Gerät zur Programmierung der jeweiligen Steuereinrichtung. Es kann sich aber auch um einen handelsüblichen Com puter handeln, der mit einer speziellen Software zur Programmierung der
Steuereinheit versehen ist. Bei den Datenleitungen kann es sich entweder um extra zur Programmierung vorgesehene Datenleitungen handeln, welche einen Schreibzugriff auf den programmierbaren Speicher erlauben. Es kann sich hierbei aber auch um Datenleitungen handeln, die auch zur Steuerung der technischen Anlage und/oder Maschine von der Steuereinheit genutzt werden, d. h. um Datenleitungen, die eine doppelte Funktion haben.

Ein Nachteil einer späteren Änderungsmöglichkeit der Steuersoftware liegt darin, dass unautorisierte Personen diese Möglichkeit missbrauchen können und beispielsweise unerlaubt den Funktions-und/oder Leistungsumfang der Steuereinheit nachträglich modifizieren und damit die gesamte techni sche Anlage bzw. Maschine"tunen". Dies hat für die Hersteller zum einen den Nachteil, dass sie durch tuning-induzierte Schäden in der Garantiezeit und damit verbundene Kosten geschädigt werden könnten. Zusätzlich kön nen nachträglich die Produktdifferenzierungsmerkmale durch unautorisierte
Personen soweit verändert werden, dass Markenpositionierung und Makenpolitik des jeweiligen Herstellers nachhaltig gestört werden.

Es ist Aufgabe der vorliegenden Erfindung, eine Steuereinheit der eingangs genannten Art derart weiterzuentwickeln, dass sie von autorisierten Instan zen jederzeit modifiziert werden kann, wobei gleichzeitig ein guter Mani pulationsschutz gegen unautorisierte Veränderungen gegeben ist.

Diese Aufgabe wird durch eine Steuereinheit gemäss Anspruch 1 gelöst. Die abhängigen Ansprüche enthalten besonders vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung.

Die erfindungsgemässe Lösung beruht hierbei auf der Kombination von zwei
Schutzkomponenten.

Zum einen wird die Steuereinheit durch das Gehäuse so gekapselt, dass ein wie auch immer geartetes Öffnen der Steuereinheit, beispielsweise durch
Aufschrauben oder Auffräsen, weitgehend dadurch verhindert wird, dass jede Öffnung der Gehäusekapselung automatisch die Zerstörung der Funk tionsfähigkeit der Steuereinheit nach sich zieht. Dies ist beispielsweise durch entsprechende Klebetechniken möglich. Es kann sich hierbei sowohl um eine
Zerstörung von wesentlichen Hardwarekomponenten als auch um eine Lö schung von zumindest für die

Funktionsfähigkeit wichtigen Softwareteilen handeln. Es ist dann nicht mehr möglich, die Einheit zu öffnen und entspre chende Speicherbausteine herauszulöten oder Codes zu analysieren, um in nerhalb der Steuereinheit vorhandene Sicherheitsmassnahmen zu analysie ren, offenzulegen oder zu umgehen und anschliessend die Steuereinheit wie der zu verschliessen und in der modifizierten Form weiterzuverwenden. Ein "Tunen"der Steuereinheit ist dann allenfalls noch über die Datenleitungen möglich.

Um dies zu verhindern, weist die Steuereinheit zum zweiten eine Kontrol leinrichtung auf, welche Schreibzugriffe, bei denen Daten über die Datenlei tungen in den programmierbaren Speicher geschrieben werden, bezüglich ihrer Berechtigung überprüft. Das heisst, jeder Prozess, der von aussen schreibend und/oder lesend über die Datenleitungen auf Daten der Steuer einheit über die Datenleitungen zugreifen möchte, muss sich einer Berechti gungskontrolle durch einen solchen"Torwächter-Prozess"unterziehen. Nur bei einer erfolgreichen Überprüfung der Berechtigung wird das Schrei ben/Lesen der Daten in bzw. aus dem programmierbaren Speicher veran lasst, d. h. die Kontrolleinrichtung lässt das Einschreiben und/oder Auslesen der Daten zu oder führt es selbst durch.

Da auf diese Weise alle Daten kanalisiert und bezüglich ihrer Authentizität überprüft werden, ist ein unerlaubtes Tuning über die Datenleitungen nicht mehr möglich. Da das Gehäuse entsprechend physisch gekapselt ist, kann dieser Prozess auch nicht unterlaufen werden.

Eine solche Kontrolleinrichtung wird vorzugsweise in Form eines Softwareprozesses innerhalb des Mikroprozessors und in dem programmierbaren Speicher selbst integriert. Alternativ ist es aber auch möglich, ein separates Sicherheitsmodul mit einer solchen Kontrolleinrichtung unabhängig vom Mikroprozessor und dem programmierbaren Speicher im Gehäuse zu plazieren und an die Datenleitungen wie eine Art Filter anzuschliessen.

Zur Durchführung der Überprüfung der Daten gibt es verschiedene generelle Möglichkeiten.

Eine Möglichkeit besteht darin, einen geheimzuhaltenden Algorithmus oder ein geheimzuhaltendes Schlüsselwort zu verwenden. Dabei wird nur dann ein Schreibzugriff zugelassen, wenn zuvor die Authentizität durch bestimmte Angaben, z. B. durch Eingabe einer PIN, oder durch eine dynamische variable Authentisierung im Rahmen eines"Challenge-Response"-Verfahrens festgestellt wurde. In einem besonders einfachen Fall weist die Kontrolleinrichtung dabei lediglich einen Speicher mit einem geheimen Kontrollwort und eine Vergleichseinrichtung auf. Es wird dann vor jedem Schreibzugriff zur Berechtigungsüberprüfung über eine Datenleitung an die Steuereinrichtung ein Schlüsselwort übermittelt und dieses Schlüsselwort mit dem Kontrollwort verglichen.

Bei einem bevorzugten Ausführungsbeispiel ist die Steuereinheit derart in dem Gehäuse eingeschlossen, dass bei einem Öffnen des Gehäuses Speicher bereiche, welche ein geheimes Kontrollwort und/oder einen geheimen
Schlüssel und/oder einen geheimen Verschlüsselungsalgorithmus enthalten, gelöscht und/oder zerstört werden, so dass es nicht mehr möglich ist, nach dem Öffnen des Gehäuses diese Daten bzw. Algorithmen auszulesen. Dies hat den Vorteil, dass beispielsweise für eine ganze Serie von Steuereinheiten dieselben geheimen Schlüssel oder Verfahren eingesetzt werden können, ohne dass die Gefahr besteht, dass eine nicht autorisierte Person eine Steuer einheit dieser Serie öffnet und dabei bewusst die Zerstörung der Funktions fähigkeit in Kauf nimmt, um so die Kenntnis der geheimen Schlüssel bzw.

Verfahren zu erlangen, die dann zum unerlaubten Modifizieren von anderen Steuereinheiten derselben Art verwendet werden können.

Bei einer anderen bevorzugten Alternative werden zur Authentisierung kei ne geheimen Algorithmen, sondern veröffentlichte bzw. veröffentlichbare kryptographische Verfahren eingesetzt. Der Authentisierungsprozess verläuft dann über den Einsatz dieser Verfahren, so dass die Sicherheit nur mehr ausschliesslich von den jeweiligen eingesetzten Schlüsseln abhängig ist.

Die Sicherheit des Gesamtsystems, d. h. desManipulationsschutzes des Steu ergeräts, wird damit auf die Sicherheit der Schlüsselmanagementprozesse verteilt. Für eine hinreichend sichere Handhabung dieser Schlüssel existieren genügend allgemein bekannte Verfahren. Die Verwendung solcher veröf fentlichbaren kryptographischen Verfahren hat den Vorteil, dass die imple mentierte Sicherheit, anders als bei geheimen Algorithmen, nicht mehr ein fach durch die Kenntnis der Algorithmen umgangen werden kann, wie dies z. B. bei einer trivialen Passworteingabe der Fall ist.

Beispiele für solche veröffentlichten kryptographischen Verfahren sind symmetrische kryptographische Verfahren wie beispielsweise DES, 3-DES oder IDEA sowie asymmetrische kryptographische Verfahren wie beispielsweise das RSA-Verfahren, bei dem der Verschlüsselungsalgorithmus auf der Arithmetik grosser Ganzzahlen beruht und die Schlüssel auf der Grundlage von zwei grossen Primzahlen erzeugt werden.

Einen besonderen Vorteil bietet die Verwendung einer solchen Steuereinheit beispielsweise zur Steuerung eines Kraftfahrzeugmotors. Bei derartigen Steuergeräten ist es auch aus verkehrssicherheitstechnischen Gründen wichtig, ein unerlaubtes Tunen der Steuerungseinheiten und damit der Motoren zu verhindern. Im Übrigen kann ein unautorisiertes Tunen hier auch zu einer frühzeitigen Beschädigung von Motoren oder Getriebe innerhalb der Garantiezeit führen, was wiederum einen grösseren Schaden für den Fahrzeughersteller bedeutet. Andererseits besteht aber auch gerade auf diesem Markt ein besonders grosses Interesse der Nutzer, sich durch entsprechendes Tunen eine höhere Leistung des Motors zu verschaffen.

Die Erfindung erlaubt bei grösstmöglicherManipulationssicherheit jederzeit gegen Vorlage und Überprüfung einer Berechtigung, beispielsweise eines elektronischen Zertifikats und/oder eines biometrischen Merkmals etc. eine Veränderung der Programmierung. Somit ist durch eine autorisierte Instanz, wie den Hersteller oder einen lizenzierten Nutzer der Steuereinheit, jederzeit eine Freischaltung, Abänderung oder ein Einspielen von diversen Inhalten wie beispielsweise Stadtplänen, Musikstücken oder dergleichen sowie eine komplette Veränderung des Programmcodes möglich.

Die mögliche Änderung von Daten oder des Programmcodes innerhalb der Steuereinheit durch eine autorisierte Person bei gleichzeitiger sicherer Ver hinderung der Manipulation hat auch den Vorteil, dass beispielsweise nur temporäre Veränderungen vorgenommen werden können, die sich nach einer vorgegebenen Zeitspanne, beispielsweise nach Ablauf einer bestimmten Zusatzlizenz, wieder selbsttätig zurücksetzen. Auf diese Weise könnte z. B. zeitlich begrenzt Leistung im Kraftfahrzeug gemietet bzw. nachgeladen werden. Ebenso könnten in Steuerungsgeräten für Navigationssysteme temporär für eine bestimmte Tour geographische Daten über die zu durchfahrenden Regionen, d. h. Stadtpläne oder Landkarten, gemietet werden, deren Daten nach Ablauf eines vorgegebenen Zeitpunkts nach Abschluss der Reise dem Navigationssystem nicht mehr zur Verfügung stehen.

Insbesondere bei Veränderungen beispielsweise der Steuerungssoftware für Kraftfahrzeuge ist es ggf. erforderlich vor Ausführung der Änderungen eine Authorisierung bzw. Freigabe durch eine dritte Stelle, beispielsweise der Kfz-Zulassungsstelle einzuholen. Zu diesem Zweck wird vor oder nach der Berechigungsüberprüfung durch die Kontrolleinrichtung eine Verbindung zu der externen authorisierenden Stelle initiiert, welche die zu installierende Steuerungssoftware freigibt.

Die Erfindung wird im Folgenden unter Hinweis auf die beigefügte Figur anhand eines Ausführungsbeispiels näher erläutert.

Die einzige Figur zeigt dabei in schematischer Blockdarstellung eine Steuereinheit 1 für einen Kraftfahrzeugmotor (nicht dargestellt).

Die Steuereinheit 1 weist zunächst ein gekapseltes Gehäuse 2 auf, in welchem sich ein Mikroprozessor mit einem programmierbaren Speicher befidet, in dem Programmdaten und Nutzdaten, unter anderem die tuningrelevanten Parameter des Motors wie der Ladedruck, gespeichert sind. Das Ge häuse 2 ist so verschlossen, dass jede Öffnung zu einer irreversiblen Zerstö rung der Funktionsfähigkeit der Steuereinheit führt. Über Datenleitungen 3,
4 ist es möglich, auf den programmierbaren Speicher zuzugreifen und die dortigen Programme bzw. Daten zu überschreiben.

Ausserdem weist die Steuereinheit 1 eine Kontrolleinrichtung 5 auf, welche als"Torwächter"alle über die Datenleitungen 3,4hereinkommenden Daten überprüft und somit jeden Schreibzugriff auf seine Authentizität hin kon trolliert.

Die Kontrolleinrichtung ist in der Figur als ein Block innerhalb der Steuer einheit dargestellt. Die Kontrolleinrichtung 5 ist in der Realität als software mässiger Prozess innerhalb des Mikroprozessors in dem programmierbaren
Speicher implementiert. Der Mikroprozessor und der programmierbare

Speicher selbst sind in der Figur nicht dargestellt.

In dem dargestellten Ausführungsbeispiel arbeitet die Kontrolleinrichtung 5 mittels einer digitalen Signatur, bei der zunächst über den gesamten Daten string, der in den Speicher geschrieben werden soll, ein Hash-Wert berechnet wird. Dieser Hash-Wert wird vor der Übermittlung über eine der Datenlei tungen 3,4 mit einem beliebigen, vorzugsweise asymmetrischen Krypto
Algorithmus, hier einem RSA-Verfahren, verschlüsselt. Das Ergebnis dieser
Berechnung wird als"Unterschrift"der eigentlichen Nachricht beigefügt, d. h. an den Datenstring angehängt.

Innerhalb der Steuereinheit 1 wird dann von der Kontrolleinrichtung 5 ver anlasst, dass über den eigentlichen Datenstring ein Hash-Wert mit dem glei chen Hash-Algorithmus wie auf der Seite des schreibenden Geräts kompri miert wird. Die angehängte digitale Signatur wird mit dem öffentlichen Schlüssel des RSA-Algorithmus entschlüsselt und der bei der Entschlüsselung enthaltene angefügte Hash-Wert der Signatur mit dem innerhalb der Steuereinheit berechneten Hash-Wert verglichen. Sind beide Werte gleich, wurde die Nachricht auf ihrem Übertragungsweg nicht verändert und von einem Gerät, welches im Besitz des richtigen geheimen Schlüssels ist, erzeugt. Die Signatur wurde damit verifiziert und die Daten authentisiert.

Falls die beiden Werte nicht übereinstimmen, wurde entweder die Nachricht oder die Signatur während der Übertragung verändert. Damit ist die Authentizität nicht mehr gegeben, und der Inhalt der Nachricht kann nicht mehr als unverändert oder von einer authentisierten Person gesendet angenommen werden. Der gesendete Datenstring wird dementsprechend von der Kontrolleinrichtung nicht akzeptiert und in der Folge nicht-wie vom Benutzer der Einrichtung zur Programmierung der Steuereinheit 1 gewünscht-in den Speicher geschrieben. Dieser Kontrollprozess ist als Programmcode links oben in der Kontrolleinrichtung 5 dargestellt. Der Datenstring selbst sowie die Bildung des Hash-Werts und der Signatur sind rechts oben innerhalb der Kontrolleinrichtung 5 dargestellt.

Da wegen der Gehäusekapselung eine Umgehung der digitalen Signatur nicht möglich ist, indem eine unbefugte Person das Gehäuse öffnet und die gewünschten Daten direkt in die jeweiligen Stellen des Speichers einschreibt, wird derManipulationsschutz an und in der Steuereinheit effektiv durch die Erfindung unterbunden. Dadurch entstehen den betroffenen Unternehmen keine unerwünschten Garantieansprüche. Die Markenstrategie der jeweiligen Unternehmen wird nicht mehr unterlaufen. Zudem wird die Lebensdauer der von der Steuereinheit angesteuerten technischen Anlagen und/oder Geräte oder Maschinen im Verhältnis zu den unerlaubt veränderten Einrichtungen erhöht. Darüber hinaus sind nachträgliche Änderungen oder Erweiterungen im Verhalten der Steuereinheit dauerhaft oder auch nur temporär jederzeit möglich, so dass eine flexible und dynamische Anpassung an sich ändernde Anforderungen von Technik, Märkten und Kunden gewährleistet werden kann.

CONTROL UNIT

Claims of **WO03001348**

Patentansprüche 1. Steuereinheit (1) mit einem Mikroprozessor, mit einem programmier baren Speicher, mit einem Gehäuse (2) und mit zumindest einer aus dem Gehäuse (2) herausführenden Datenleitung (3,4) zur Verbindung mit einer externen Einrichtung zum Schreiben und/oder Lesen von Da ten in bzw. aus dem programmierbaren Speicher, dadurch gekennzeichnet, dass die Steuereinheit(1) derart in dem Gehäuse (2) eingeschlossen ist, dass bei einem Öffnen des Gehäuses (2) die Funktionsfähigkeit der Steuereinheit(1) zumindest teilweise zerstört wird, und dass die Steu ereinheit(1) eine Kontrolleinrichtung (5) aufweist, welche einen
Schreib-und/oder Lesezugriff, bei dem Daten über die Datenleitung (3,
4) in den programmierbaren Speicher geschrieben oder aus diesem ge lesen werden, bezüglich einer Berechtigung überprüft und nur bei er folgreicher Überprüfung der Berechtigung das Schreiben/Lesen der Daten in bzw. aus dem programmierbaren Speicher veranlasst.

2. Steuereinheit nach Anspruch1, dadurch gekennzeichnet, dass die
Kontrolleinrichtung einen Speicher mit einem geheimen Kontrollwort und eine Vergleichseinrichtung umfasst, um ein vor einem Schreibzu griff über eine Datenleitung an die Steuereinrichtungübermitteltes Schlüsselwort mit dem Kontrollwort zur Berechtigungsüberprüfung zu vergleichen.

3. Steuereinheit nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Kontrolleinrichtung Mittel zur Durchführung eines Challenge
Response-Verfahrens zur Berechtigungsüberprüfung umfasst.

4. Steuereinheit nach einem der Ansprüche 1 bis 5, dadurch gekenn zeichnet, dass die Kontrolleinrichtung Mittel zur Verschlüsselung und/oder Entschlüsselung von Daten umfasst.

5. Steuereinheit nach einem der Ansprüche 1 bis 3, dadurch gekenn zeichnet, dass die Kontrolleinrichtung (5) Mittel zur Überprüfung einer digitalen Signatur der über die Datenleitung (3,4) übermittelten Daten umfasst.

6. Steuereinheit nach einem der Ansprüche 1 bis 5, dadurch gekenn zeichnet, dass die Steuereinheit derart in dem Gehäuse eingeschlossen ist, dass bei einem Öffnen des Gehäuses Speicherbereiche, welche ein geheimes Kontrollwort und/oder einen geheimen Schlüssel und/oder einen geheimen Verschlüsselungsalgorithmus enthalten, gelöscht und/oder zerstört werden.

7. Steuereinheit nach einem der Ansprüche 1 bis 6, dadurch gekenn zeichnet, dass die Kontrolleinrichtung (5) Mittel zur Aufnahme einer
Verbindung zu dritten Stellen enthält und ein Schreib-/Lesezugriff nur zugelassen ist, wenn eine Freigabe durch diese dritte Stelle erfolgt ist.

8. Verwendung einer Steuereinheit (5) nach einem der Ansprüche 1 bis 7 zur Steuerung eines Kraftfahrzeug-Motors.
